Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

The Information Commissioner's response to the public consultation from the Department for Business, Enterprise and Industrial Strategy (BEIS): *Delivering a smart and secure electricity system: consultation on interoperability and cyber security of energy smart appliances and remote load control.*

About the ICO

1. The Information Commissioner's Office (ICO) welcomes the opportunity to respond to the BEIS consultation *Delivering a smart and secure electricity system: consultation on interoperability and cyber security of energy smart appliances and remote load control* (the consultation).

2. The ICO has responsibility for promoting and enforcing data protection and information rights. This includes responsibilities under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA), the Freedom of Information Act 2000 (FOIA), the Network and Information Systems Regulations 2018 (NIS), the Environmental Information Regulations 2004 (EIR) and the Privacy and Electronic Communications Regulations 2003 (PECR). The ICO is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO provides guidance and support to individuals and organisations, aimed at helping organisations to comply, and it takes appropriate action when needed.

Data protection and ESAs

3. Energy Smart Appliances (ESAs) can help consumers manage their homes, monitor the energy they use and reduce waste. They can also bring reductions in household bills and greater convenience. Developments in ESAs also hold the potential for the development of new products and services, driving innovation and contributing to economic growth.

4. While each ESA will have different characteristics and technologies, according to their purpose, in general, ESAs will involve the generation, transmission and analysis of data relating to consumers by a broad range of organisations. This data might include detailed information about energy consumption, patterns of use and the nature of households, including inferences about the presence or absence of people.

5. The volume of this data and need for detailed analysis is likely to increase as more people use ESAs. Moreover, there may be incentives which encourage more sharing. The potential for consumers to integrate ESAs into increasingly interoperable smart home setups in future is also likely to add further complexity and risk.

6. Data protection ensures that organisations process personal data fairly, lawfully and transparently, as they realise these opportunities. It provides a framework that gives people trust and confidence in how organisations will use their data, and ensures that organisations respect individual rights and mitigate risks of harm. The risk-based approach of the data protection framework relies on foundational principles[1], irrespective of the technologies used, rather than adopting a prescriptive approach.

7. Data protection by design means building in privacy and data protection requirements at the earliest design stage of ESAs and plans for their regulation. It also means considering these requirements throughout the ESA life cycle, including circumstances when an ESA might pass into new hands.

8. Integrating privacy from the start will help inform ESA standards and specifications, ensuring that ESAs are safe and secure. This is likely to be particularly important in the context of the proposals to mandate 'smart' functionality. A data protection by design approach will positively influence a privacy-first approach to future innovation in ESAs.

9. For these reasons, all developments relating to ESAs should factor in requirements for data protection and data privacy at the outset, and in the 'short-term'[2] onwards. In particular, government should ensure that it does not defer consideration of these factors to a later stage especially as it may then be more difficult to integrate the necessary safeguards and protections into existing ESA frameworks and systems.

10. While the consultation includes refrigeration, it specifically excludes other consumer ESA devices, including other whitegoods. As functionality and uptake of these appliances increases, it will be important to consider how related regulations that apply to connected whitegoods, such as those

[1] The principles | ICO
[2] Table 2 in the consultation

outlined in the Product Security and Telecommunications Infrastructure Bill, will interact with these proposals.

Older people, people with disabilities and other vulnerable groups

11. Older people and people with disabilities may particularly benefit from the use of smart technologies, for example ESAs that might help in managing or reducing their heating bills. Other benefits may emerge as ESAs develop into other areas of domestic life. It will be important to strike the right balance between achieving these outcomes while also ensuring that the ESAs and the surrounding networks respect privacy. In this respect, the context in which people use ESAs will be a relevant consideration, for example, taking into account that some people in social housing or in shared rented accommodation may not own the ESAs in their home or control the accounts linked to them.

12. ESA design needs to ensure that people are not excluded, so that, for example, that older people or those with disabilities can use ESAs. In this context, it will be important to recognise that people's right to privacy does not diminish because of their position of vulnerability. People will need to be able to exercise their rights and be informed about the ESA in a way which is suitable to their circumstances. The processing of personal data needs to be fair; include measures for people who don't have access to digital solutions; and not lead to any discrimination against minority or marginalised groups.

Data protection

Personal data

13. Scoping out the personal data that organisations will process when developing and supplying ESAs should take place at an early stage. Where data relating to the use of domestic ESAs links to the data of an individual, it will be personal data. For example, even where a supplier uses a unique identifier rather than a name or address, the data will still be personal data when it is inextricably linked to the individual account holder. Data processed by, for example, apps on personal devices will also be personal data. Any information collected from ESAs is 'observed' data, as it arises from the use of the ESA. Analysis of that data, or 'inferred' data, may also be personal data if it allows for the identification, directly, or indirectly, of a natural person.

Data portability

14. Individuals have the right to ask for organisations to port their personal data between different services or providers[3]. The intent behind this right is to allow individuals to switch providers easily, or to request that controllers transmit the data directly to other controllers.

15. The right to data portability applies where the processing is based on consent or contract and is undertaken by automated means and will therefore apply to the use of ESAs. Importantly however, data portability applies only to personal data that has been provided to the controller by the individual – so in the context of ESAs, this would not necessarily include all personal data relating to account holders. The right applies to data actively and knowingly supplied by the data subject (such as name and address) and data observed by the controller based on the data subject's use of the service. However, inferred data, perhaps generated following an analysis of the observed data, is not in scope of the right to portability, although such data may still be covered by the right of access.

16. Organisations in ESA networks will therefore need to understand and distinguish between different types of data in order to ensure that they can support individuals in exercising their rights.

Transparency

17. Greater use of ESAs is therefore likely to lead to a considerable increase in the processing of personal data. While the risks of the technologies that ESAs use may not be new in character, they are likely to aggravate existing risks, particularly as use of ESAs may lead to increased surveillance and profiling, invisible processing, and automated decision making (for example, regarding energy tariffs).

18. Transparency is a fundamental principle of data protection law. Organisations should be clear, open and honest with people about who they are, as well as how and why they want to use personal data. The regulatory framework for ESAs needs to underpin the need for transparency so people can understand what data the ESA may process, who is doing this, and why, for each device and service. In particular, it should encourage designers and developers to look at suitable methods

[3] Article 20 UK GDPR

for communicating privacy information to ESA users, given the potentially limited nature of the user interface in an ESA.

19. As part of their approach to transparency, organisations will need to be able to explain to individuals how they use artificial intelligence in relation to the ESA, including the inferences the organisation will draw from the individual's personal data. The ICO has published a range of blogs and resources in relation to its AI auditing framework which is likely to be helpful in this respect.[4]

20. Organisations in an ESA network will also need to be able to explain the nature of any tracking or profiling that might take place and the safeguards they will put in place to protect consumers. Transparency is essential where there will be automated individual decision making and profiling. Individuals have additional protections in these situations, and organisations can only carry out solely automated decision making that has a legal or similarly significant effect on them in certain limited circumstances.[5] In such cases, organisations will need to give people information about the processing and simple ways to request human intervention or challenge a decision.

Consent

21. Where consent is the lawful basis for processing, organisations need to ensure that they give people genuine choice and control over how these organisations will use the personal data[6]. If ESAs are required to have smart functionality, this includes giving consumers a choice about whether or not to participate in the ESA network. This choice needs to be a real, transparent choice, ensuring that the request for consent is not bundled up with other terms and conditions in ways that are difficult to understand, or which could be overlooked. Adopting and implementing appropriate standards – such as BSI standard PAS 1878 which prescribes that ESAs should have the facility to enable and disable the 'energy smart' functionality - will help to provide real choices for consumers.

[4] AI Auditing Framework | ICO
[5] Article 22 UK GDPR - Rights related to automated decision making including profiling | ICO
[6] Consent | ICO

Fairness

22. Processing of personal data needs to be fair and this means that organisations should only handle personal data in ways that people would reasonable expect. Personal data from ESAs can provide detailed insights into people's lifestyles and habits. Collection and processing of such personal data could be unfair if it is not transparent or if organisations keep it for longer than they need to.

23. Fairness is not only about how organisations process the personal data, but also about the outcome of that processing, and the impact it may have on people. People should also be able to expect that organisations will not use their personal data in ways that have unjustified adverse impacts on them.

Necessity and proportionality

24. Organisations deploying ESAs will also need to consider whether what they want to do is necessary and proportionate, and whether any less intrusive means exist to achieve their purpose. Data protection law does not stand in the way of the use of ESAs, but organisations need to consider how they can achieve their aims, while also upholding information rights.

Accountability

25. Data protection law requires organisations to be accountable for the processing of personal data they carry out. This means they are able to demonstrate how they comply with the data protection principles and help people exercise their rights.

26. ESAs will involve potentially complex networks, with multiple participants involved in different parts of the data processing by an ESA. This can make it difficult for individuals to know who is processing their data, for what purpose, and how they can exercise their rights. The use of 'privacy-friendly defaults' will therefore be an important aspect in the process of communicating this information to device users.

Anonymisation and privacy preserving techniques

27. Anonymisation offers an alternative way to use or share data by making sure that individuals are not identifiable. Pseudonymisation involves replacing personal identifiers like a name with a reference number, making it more difficult to attribute it to a specific individual. Adopting such an approach enables and supports innovation, helping organisations to mitigate risks. We have developed anonymisation guidance which will be a useful guide to organisations working in this space[7].

28. Using suitable privacy enhancing technologies (PETs) can also enable the sharing and use of data in a privacy-preserving way, particularly when organisations are looking at analysing the data for broader insights and are not concerned with the individual's personal data. PETs refer to a range of technologies but techniques that might be appropriate in the development of ESAs, depending on the circumstances, could include:

    - Privacy preservation via aggregation – where data is aggregated by way of groupings before it is disclosed to an ESA provider or other participants in the ESA network who seek to derive insights from it, which theoretically serves to increase the privacy of individuals without degrading the utility of the data
    - Privacy preservation via encryption – where data is subject to encryption techniques that allow computation to be run on an encrypted dataset
    - Privacy preservation via 'noise' – where noise data (ie meaningless additional information) is added to the data in accordance with specific criteria, concealing the device data whilst allowing insights to be derived.

29. Using anonymisation or pseudonymisation techniques and considering the use of PETs can help reduce the risks of processing. It is therefore particularly important to consider how these techniques might address risks in processing throughout the lifecycle of an ESA. This can be especially significant if, now or in the future, the personal data also includes special category data, for example because it relates to an individual's health.

[7] ICO call for views: Anonymisation, pseudonymisation and privacy enhancing technologies guidance | ICO

30. Re-identification is a risk that government will need to consider if it intends to release open data for analysis. Large data sets of aggregate information, based on the personal data of individuals might reveal direct or indirect identifiers or other sensitive attributes. Government will therefore need to conduct a benefit/risk assessment to ascertain the risk of linking any published data sets to other data sets, if this should arise.

Data protection impact assessments

31. Controllers should undertake data protection impact assessments (DPIAs)[8] to help to identify and minimise the data protection risks arising from the future use and regulation of ESAs. Carrying out DPIAs will also support a data protection by design and default approach. Controllers **must** undertake a DPIA in certain specific circumstances, for example, where the proposals involve new technology and is likely to produce a high risk to an individual's rights and freedoms, or where there is systematic and extensive profiling with significant effects.

32. Mapping and detailing the anticipated data flows at the start of the design phase in a DPIA will help to clarify the roles and responsibilities of each participant in the network by, for example, working through what each will have sight of and the extent to which it will be personal data. This, in turn, will provide an overview of risk and allow for both a holistic and more granular approach to mitigating steps, which will help in avoiding complications later.

33. When considering the data protection and cyber security aspects of ESA design, including how to minimise data sharing with third parties, it will also be important to consider that consumers may choose to integrate ESAs into wider, increasingly connected and interoperable 'smart home' setups, or may choose an ESA that links with a smart voice assistant. This has the potential to add further complexity to ESA data flows and management of cyber security risks. For example, in some setups, individual devices from different manufacturers may be linked to different cloud servers, or in others, smart home systems may be designed to process data at the 'edge',[9] with minimal transfer of data to the cloud.

[8] Data protection impact assessments | ICO

[9] The 'edge' in edge computing describes where data processing takes place near the source of the data

Controllers and processors

34. The responsibility of controllers, the requirements of data processors and the position of joint controllers[10], together with the lawful basis for processing on which each relies, will be relevant to the deployment of ESAs. Each participant, including government, regulators, manufacturers or software developers, will have their own part to play in the overall network. Each may process personal data for different purposes and therefore may rely on different lawful bases for doing so.

35. Importantly, even if one party intends to process aggregate information, this does not exclude them from data controllership, if they were only able to obtain that information by means of another party processing the original personal data.

36. The design and development process therefore needs to factor in controller and processor responsibilities and ensure that appropriate contractual arrangements set them out. Government will also need to take these responsibilities into account when establishing frameworks for regulation and assurance.

Data sharing and privacy

37. In view of the complexities and potential for extensive data sharing, organisations in ESAs networks will find the ICO's data sharing information hub, which includes the ICO's data sharing code, a valuable resource.[11] In addition, it may be helpful to consider the adoption of appropriate common standards and devising privacy frameworks that do not replace data protection legislation but help in supporting and assuring privacy and in ensuring that those involved in ESA networks follow best practice, as is the case for Smart Meters.[12]

[10] Articles 24,28 and 26 respectively UKGDPR

[11] Data sharing information hub | ICO

[12] Smart Metering Implementation Programme: Review of the Data Access and Privacy Framework (publishing.service.gov.uk)

Security

38. Organisations need to process personal data securely by means of 'appropriate technical and organisational measures'.[13] This includes ensuring that personal data is protected from accidental loss, destruction or damage and includes the need for cyber, physical and organisational security. The consultation discusses energy security which also touches on these areas. The security principle will be a key consideration in the development and regulation of ESAs.

39. Any security threats to ESA systems will have the potential to affect the confidentiality, integrity and availability of the services provided. The cyber-attacks cited in the consultation are examples where bad actors seek to disrupt services and adversely impact on wider society, but this impact is compounded when ransomware also targets personal data. Sharing personal data between parties also increases the chances of a supply-chain vulnerability. For example, malicious code could compromise the ESAs and the network they are linked to, and could open access to cloud based services and cause network disruption. As a consequence, cyber security measures need to address the potential for ESA devices and other parts of the network cascading adverse consequences.

40. Use of wireless communications may make also ESAs vulnerable to physical and eavesdropping attacks. Security requirements should therefore include security controls such as encryption of sensitive data, checks on the validity of critical commands sent within the system and tamper resistance of ESA equipment.

41. Potential weaknesses could arise from individual ESAs, as well as the IT infrastructure of the suppliers and the communication networks. The potential for such vulnerabilities means that appropriate technical and organisational measures should apply to the whole process. This will need to include any in-home elements of the network, the transmission of personal data across the network and the storage and processing of personal data by suppliers, networks and other data controllers, to ensure protection of personal data. Mechanisms for securing personal data in-use, data in-transit and data at-rest will be critical in defending against cyber-attacks that target personal data. Consideration should also be given to the

[13] UK GDPR, Article 5(1)(f) and Article 32.

risks posed by legacy devices, or in more integrated smart homes that process data in the cloud, or in the future, on the 'edge'.

42. Technical and organisational measures also need to protect the personal data from other threats, such as the potential for unauthorised disclosure, for example, when if an individual sells or hands over their ESA to someone else.

43. Security and prevention of cyberattack cannot therefore be viewed in a vacuum. The protections that come from the adoption of and compliance with appropriate standards must be integrated into other security measures that protect the entire network as well as individual organisations, and should include the use of any common systems.

44. We therefore welcome the continued promotion of NIS and the Cyber Assessment Framework (CAF) as a common strategic approach to the UK cyber sector, together with the adoption and implementation of standards such as ETSI 303 646 and PAS 1848 to address security and other risks. However, while these provisions will address some vulnerabilities, risks might remain where some ESAs are not required to comply. Security assessments will also need regular review to meet emerging threats, given the potential for cyber-attacks across the entire network.

NIS Regulations

45. It is important to note that if a network is established by a public authority or a group of them, or by a mixture of public and private organisations, they may qualify as a digital service provider under NIS. However, it will be for government to decide which load controllers should be subject to the NIS regulations, and the threshold requirements of remote load control that they should apply.

46. As mentioned in the consultation, BEIS and the Office for Gas and Electricity Markets (Ofgem) are joint competent authorities for the electricity subsector under the NIS regulations. The ICO is the competent authority under the NIS regulations for relevant digital service providers (RDSPs) and also has a regulatory function over RDSPs and Operators of Essential Services (OES) wherever those organisations are processing personal data. This is because, in many cases, OES and RDSPs will be data controllers and therefore data protection law also applies to them

47. Cross regulatory cooperation is likely to be particularly relevant for cloud services. For example, this might arise if a load controller uses cloud-based Infrastructure-as-a-Service (IaaS), or if a cloud service provider (CSP) hosts an application to manage ESAs for a supplier or end user. We also envisage that critical dependencies could emerge for OES under BEIS supervision, where for example load controllers rely on cloud services subject to the current regulations and supervision by the ICO. Such dependencies will potentially increase should Managed Service Providers (MSPs) also come into scope for the ICO under the proposed changes to the NIS regulations. Regulators will need clarity about their respective responsibilities for proactive assurance and reactive investigations.

48. The consultation also highlights the potential involvement of some organisations which provide a demand side response (DSR) service but will not fall within the proposed thresholds for NIS. Given the potential for any attack to threaten the entire network, we consider that the requirements for cyber security should be no less robust than for other organisations, as any weakness could compromise other parts of the network.

49. We recognise the importance of cross-regulatory cooperation and alignment in relation to ESAs to avoid the potential burden of dual oversight for OES and RDSPs. We also welcome the proposed collaborative approach between government and industry in formulating risk assessments and cyber security requirements in relation to future systems of ESAs and DSR. We look forward to engaging further with government, regulators and other relevant stakeholders in building suitable governance frameworks to support the regulation of ESAs.

Smartphone apps and PECR

50. The consultation suggests that consumers will interact with ESAs and DSR service providers via smartphone apps to access tariff related options. If this is the case, ESA manufacturers and permitted third party providers or other suppliers will need to ensure that these developments do not introduce new vulnerabilities into the system.

51. Where an organisation uses technology that stores or accesses information on a user's device or equipment, then Regulation 6 of PECR will apply. Regulation 6 will therefore apply to any smartphone or tablet used in

conjunction with an ESA, as well as the ESA itself, where that functionality exists[14].

52. Where Regulation 6 PECR applies, the user must receive clear and comprehensive information about the storage or access (in line with UK GDPR requirements), together with an appropriate consent mechanism, unless an exemption applies.

53. Regulation 6 contains only two exemptions from this requirement. These are where the storage or access is necessary for the transmission of a communication or where the storage or access is 'strictly necessary' for the provision of an online service explicitly requested by the user or subscriber. It may be possible for the organisations requiring storage or access for the use of ESAs to rely on one of these exemptions, but they will need to be able to justify why this is the case.

54. It is equally important to note that Regulation 6 requires **consent** for the storage or access, and that it applies **whether or not** the information is personal data. This means that whoever is storing information, or accessing information stored, cannot rely on an alternative lawful basis under the UK GDPR (such as legitimate interests).[15]

55. If a smartphone or tablet app includes any marketing functionality then Regulation 22 of PECR will apply, for example, if the user receives an electronic communication about a discounted tariff. Specific consent is required in most cases to send unsolicited direct marketing messages and developers will need to build in mechanisms to allow the consumer to opt out of receiving them.[16]

Consultation

56. We welcome the opportunity for early engagement on the further development of ESAs and the surrounding frameworks. We have received a request for consultation in relation to the primary legislation, but the requirements for consultation under article 36(4) UK GDPR will arise afresh for any regulations proposed under the Bill, once enacted.

[14] Guidance on the use of cookies and similar technologies | ICO
[15] Guidance on the use of cookies and similar technologies | ICO
[16] Electronic and telephone marketing | ICO